

Corre voce che i cinesi abbiano trovato il modo per infrangere la codifica crittografica Sha-1, ma in realtà si tratta di una verità parziale: il codice è violabile in tempi da ere geologiche. Dunque la strada è praticamente inutile

«Terrorismo tecnologico sulla e-firma»

La firma digitale disciplinata dalle norme italiane vanta un livello di sicurezza altissimo immutato da dieci anni

PIERLUIGI RIBOLFI

Corre voce che la firma digitale non sia più sicura. Sembra infatti che all'università di Shandong, in Cina, abbiano trovato un modo per "rompere" la codifica Sha-1, componente fondamentale del sistema crittografico: pertanto, si dice, prima o poi qualunque documento firmato digitalmente potrebbe essere alterato senza che il ricevente se ne possa accorgere. È solo questione di tempo. Detta così, la conclusione fa rizzare i capelli. Qualcuno poi cita anche l'art. 31 del Codice sulla Privacy, che stabilisce obblighi di sicurezza "in relazione alle conoscenze acquisite in base al progresso tecnico", ipotizzando pertanto, in caso di accessi dolosi, responsabilità soggettive anche penali. Per comprendere realmente cosa potrebbe succedere, occorrono alcune considerazioni tecniche. La firma digitale prevede due fasi. Nella prima il documento digitale da firmare viene compresso o dilatato, secondo un processo matematico ben preciso - denominato Sha-1 - in una sequenza di lunghezza fissa (160 bit), chiamata "impronta". Nella seconda l'impronta viene trasformata con un geniale algoritmo - denominato Rsa - in un'altra sequenza (di 1024 bit), e questa è la "firma". L'algoritmo opera con due chiavi diverse, una per cifrare, l'altra per decifrare, differenti per ogni firmatario. L'algoritmo Rsa utilizza chiavi derivate da una coppia di numeri primi che sono utilizzati in modo complementare per le operazioni di cifratura e decifratura. In sintesi la chiave privata, che serve a cifrare, è basata sui due numeri primi, mentre la chiave pubblica, che serve per decifrare, è basata sul loro prodotto.

Se si riuscisse, a partire dalla chiave pubblica, a trovare i due numeri che costituiscono la base di calcolo della chiave privata, un abile informatico malintenzionato potrebbe sostituire il documento originale, cifrarlo con la chiave "giusta" ricavata dai due numeri e sostituirlo all'altro. Nessuno se ne accorgerebbe. Ma non è così facile scomporre il

prodotto nei suoi due fattori: con le tecniche attuali di firma si utilizzano numeri primi grandissimi, ognuno lungo 1024 bit, pari a circa 330 cifre decimali. Poiché non esiste altro modo di scomporre il numero se non per tentativi, il tempo occorrente per fare ciò, anche con i più potenti calcolatori, sarebbe maggiore dell'età dell'universo. Pertanto, a meno che non si trovino nuove tecniche di scomposizione, i tempi richiesti, anche utilizzando migliaia di calcolatori in parallelo, sarebbero tali da rendere praticamente impossibile quest'operazione.

Come si è detto, l'Sha-1 è un processo complicatissimo che trasforma qualunque documento in una sequenza di 160 bit. Data l'impronta non è possibile risalire al documento che l'ha generata. Al massimo, operando per tentativi si potrebbe ricavare un documento che abbia la stessa impronta, che, ovviamente, non avrà nulla a che vedere con quello originale: anzi, probabilmente sarà una sequenza di bit a caso, senza senso.

Cosa sono riusciti a fare i matematici cinesi? Hanno trovato un metodo un po' più intelligente di quello brutale per tentativi, che, data un'impronta, riesce a trovare un documento "origine". Ma il numero di operazioni sufficienti per arrivare all'origine resta elevatissimo. Ma la sostanza resta la medesima: il tempo necessario per arrivare al risultato è troppo. Dunque la questione non si pone. Non solo. Se anche si riuscisse in futuro "rompere" con minori difficoltà la codifica Sha-1, resterebbe ancora da infrangere la seconda fase, quella che vede appunto l'impronta cifrata con le due chiavi. E qui non c'è nessuno, né in Cina né altrove, che al momento si sia detto in grado di cantare vittoria: infatti, il problema di scomporre il prodotto di due numeri primi nei suoi due fattori non ha trovato una soluzione veloce, né se ne vedono all'orizzonte.

La conclusione è che la firma digitale, così come disciplinata dalle norme italiane (Sha-1 + Rsa), vanta un livello di sicurezza altissimo, che è rimasto di fatto immutato dal momento che è stato adottato ormai

dieci anni fa.

Pertanto, affermare che la firma digitale non è più sicura significa fare del terrorismo tecnologico, di cui proprio non si sente il bisogno, soprattutto in questa fase di ampia diffusione di questa tecnologia, voluta dal Codice dell'Amministrazione digitale e dalle norme fiscali. Per quanto poi riguarda le invocate responsabilità penali per "mancato aggiornamento", il problema non si pone proprio. Il **Cnipa** (Centro Nazionale per l'Informatica nella Pubblica amministrazione), che ha il compito di indicare le regole tecniche in materia, sta seguendo con la massima attenzione l'evoluzione delle tecnologie e quando sarà necessario, non mancherà di proporre l'aggiornamento delle regole attuali: il risultato cinese - ma non solo quello - è ben noto e viene tenuto dagli esperti nella dovuta considerazione. Ma, per certo e in ogni caso, nessuno potrà comunque essere giudicato colpevole per aver osservato le regole oggi vigenti. ■

() Docente di informatica nell'Università di Bologna, già componente del Collegio del Cnipa, presidente della Commissione interministeriale per la dematerializzazione.*